jc929 U.S. PTO 09/800505 03/08/01

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-171619
(43)Date of publication of application : 30.06.1997

(51)Int.Cl. G11B 7/00
G06F 12/14
G09C 1/00
G11B 7/007
G11B 11/10
G11B 20/10
// H04L 9/10

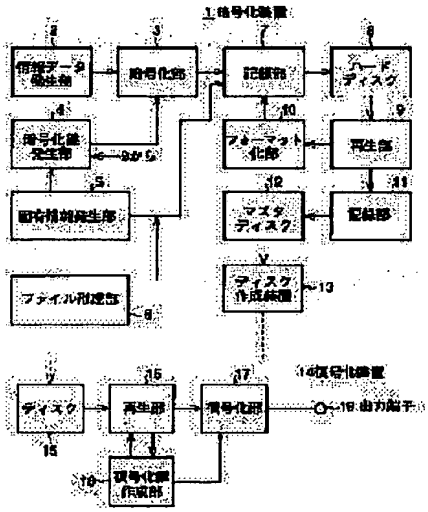
(21)Application number : 08-095004
(22)Date of filing : 17.04.1996

(71)Applicant : SONY CORP
(72)Inventor : ISHIGURO RYUJI
MINAMI MASAFUMI

(30)Priority
Priority number : 07267252 Priority date : 16.10.1995 Priority country : JP

(54) METHOD AND DEVICE FOR CIPHERING AND METHOD AND DEVICE FOR DECIPHERING

(57)Abstract:
PROBLEM TO BE SOLVED: To impose secure protection.
SOLUTION: A ciphering key generation part 4 generates a ciphering key on the basis of information characteristic of a recording medium supplied from a characteristic information generation part 5, a ciphering part 3 ciphers information to be recorded on the recording medium with the ciphering key to make a master disk 12, and a disk 15 is made finally. A reproduction part 16 reproduces the disk 15, a deciphering key generation part 18 generates a deciphering key from the reproduced data, and a deciphering part 17 deciphers the ciphered data reproduced by the reproduction part 16 according to the deciphering key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－171619

(43)公開日　平成9年（1997）6月30日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ１１Ｂ	7/00		9464－5D	Ｇ１１Ｂ	7/00	Ｑ
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14 ３２０	Ｂ
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00 ６６０	Ｄ
Ｇ１１Ｂ	7/007		9464－5D	Ｇ１１Ｂ	7/007	
	11/10	５１１	9075－5D		11/10 ５１１	Ｄ

審査請求　未請求　請求項の数25　ＯＬ（全 16 頁）　最終頁に続く

(21)出願番号　特願平8－95004

(22)出願日　平成8年（1996）4月17日

(31)優先権主張番号　特願平７－２６７２５２

(32)優先日　平7（1995）10月16日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(72)発明者　石黒　隆二
東京都品川区北品川6丁目7番35号　ソニー株式会社内

(72)発明者　南　雅文
東京都品川区北品川6丁目7番35号　ソニー株式会社内

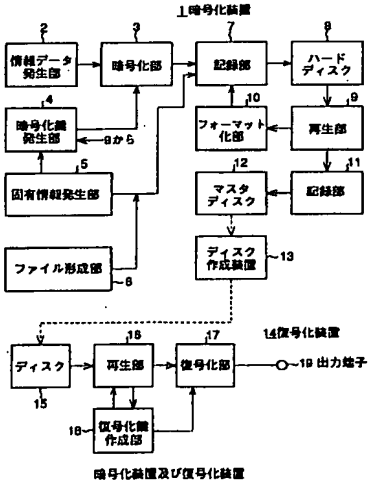
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】暗号化方法および装置並びに復号化方法および装置

(57)【要約】

【課題】　強力なコピープロテクトを掛けることができるようにする。

【解決手段】　固有情報発生部５より供給される記録媒体に固有の情報に基づいて、暗号化鍵発生部４は暗号化鍵を発生し、暗号化部３はその暗号化鍵によって記録媒体に記録すべき情報を暗号化し、マスタディスク１２が作成され、最終的にディスク１５が作成される。再生部１６によりディスク１５が再生され、再生データから復号化鍵作成部１８により復号化鍵が作成され、復号化部１７によりその復号化鍵に基づいて再生部１６によって再生された、暗号化された再生データが復号化される。



1

【特許請求の範囲】

【請求項1】　記録媒体に固有の固有情報に基づいて暗号化鍵を作成し、前記暗号化鍵に基づいて、前記記録媒体に記録すべき情報を暗号化する暗号化方法において、前記記録媒体に固有の前記固有情報は、前記記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分の周波数であることを特徴とする暗号化方法。

【請求項2】　前記記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分を示すファイルは、暗号化された前記情報のファイルとともに、前記記録媒体に記録されることを特徴とする請求項1に記載の暗号化方法。

【請求項3】　記録媒体に固有の固有情報に基づいて暗号化鍵を作成し、前記暗号化鍵に基づいて、前記記録媒体に記録すべき情報を暗号化する暗号化方法において、前記記録媒体に固有の前記固有情報は、前記記録媒体に記録されるべき暗号化された前記情報の所定の部分に挿入されるランダムデータであることを特徴とする暗号化方法。

【請求項4】　前記ランダムデータは、ＩＳＯ９６６０規格の通常のファイルとして前記記録媒体に記録されることを特徴とする請求項3に記載の暗号化方法。

【請求項5】　前記ランダムデータは、インタリーブされたファイルとして前記記録媒体に記録されることを特徴とする請求項3に記載の暗号化方法。

【請求項6】　前記ランダムデータは、マルチエクステントされたファイルとして前記記録媒体に記録されることを特徴とする請求項3に記載の暗号化方法。

【請求項7】　前記ランダムデータは、ＩＳＯ９６６０規格のファイルのプリギャップエリアに記録されることを特徴とする請求項3に記載の暗号化方法。

【請求項8】　前記ランダムデータは、ＩＳＯ９６６０規格のファイルのシステムエリアに記録されることを特徴とする請求項3に記載の暗号化方法。

【請求項9】　前記ランダムデータは、ＩＳＯ９６６０規格のファイルのプライマリボリュームディスクリプタのアプリケーションエリアに記録されることを特徴とする請求項3に記載の暗号化方法。

【請求項10】　前記ランダムデータは、前記記録媒体の表面に記録されることを特徴とする請求項3に記載の暗号化方法。

【請求項11】　前記ランダムデータは、所定の疑似ランダム発生器によって作成されたランダムファイルの所定の部分から選択されたランダムデータであることを特徴とする請求項3に記載の暗号化方法。

【請求項12】　前記ランダムデータからなる前記ランダムファイルの前記所定の部分を示すファイル、および前記ランダムファイルは、暗号化された前記情報のファイルとともに、前記記録媒体に記録されることを特徴とする請求項11に記載の暗号化方法。

2

【請求項13】　前記暗号化された前記情報のファイルおよび前記記録媒体に記録されるべき暗号化された前記情報の所定の部分に挿入されるランダムデータの中の所定の部分を示すファイルを前記記録媒体に記録することを特徴とする請求項3に記載の暗号化方法。

【請求項14】　前記記録媒体に固有の前記固有情報は、前記記録媒体の表面に記録されることを特徴とする請求項3に記載の暗号化方法。

【請求項15】　記録媒体の固有の情報から作成した第1の暗号化鍵と前記第1の暗号化鍵とは独立の第2の暗号化鍵から第3の暗号化鍵を作成し、
前記第3の暗号化鍵によって、前記記録媒体に記録すべき情報を暗号化することを特徴とする暗号化方法。

【請求項16】　記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるべきランダムデータに基づいて作成された暗号化鍵によって暗号化された前記情報が格納された第1のファイル、および暗号化された前記情報の所定の部分に挿入される前記ランダムデータの所定の部分を示すデータが格納された第2のファイルが記録された前記記録媒体から、前記第1のファイル、および前記第2のファイルを再生し、
再生された前記第2のファイルに格納された、前記ランダムデータの所定の部分を示すデータに基づいて、再生された前記第1のファイルに格納された暗号化された前記情報から、前記ランダムデータを検出し、
検出された前記ランダムデータから復号化鍵を作成し、
前記復号化鍵によって、再生された前記第1のファイルの暗号化された前記情報を復号化することを特徴とする復号化方法。

【請求項17】　記録媒体に記録されるべき情報の所定の部分のウォブリング周波数に基づいて作成された暗号化鍵によって暗号化された前記情報が格納された第1のファイル、および前記記録媒体に記録されるべき暗号化された前記情報の所定の部分を示すデータが格納された第2のファイルが記録された前記記録媒体から、前記第1のファイル、および前記第2のファイルを再生し、
再生された前記第2のファイルに格納された、暗号化された前記情報の所定の部分を示すデータに基づいて、再生された前記第1のファイルに格納された前記情報の所定の部分のウォブリング周波数を検出し、
検出された前記ウォブリング周波数に基づいて、復号化鍵を作成し、
前記復号化鍵によって、再生された前記第1のファイルに格納された、暗号化された前記情報を復号化することを特徴とする復号化方法。

【請求項18】　記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分の周波数に基づいて作成された暗号化鍵によって暗号化された前記情報が格納された第1のファイル、および前記記

録媒体に形成されるべきウォブリングされたプリグループまたはランド部の所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、前記第１のファイルおよび前記第２のファイルを再生し、
再生された前記第２のファイルに格納されたウォブリングされたプリグループまたはランド部の所定の部分を示す前記データに基づいて、前記記録媒体に形成された前記プリグループまたはランド部の所定の部分のウォブリング周波数を検出し、
検出された前記ウォブリング周波数に基づいて、復号化鍵を作成し、
前記復号化鍵によって、再生された前記第１のファイルに格納された暗号化された前記情報を復号化することを特徴とする復号化方法。

【請求項１９】　所定の記録媒体に記録された、所定の疑似ランダム発生器によって作成されたランダムデータからなるランダムファイルの所定の部分から選択された前記ランダムデータに基づいて作成された暗号化鍵によって暗号化された情報が格納されたファイル、前記ランダムデータからなる前記ランダムファイルの所定の部分を示すデータが格納されたファイル、および前記ランダムファイルを再生し、
再生された前記ランダムファイルの所定の部分を示すデータが格納された前記ファイルに基づいて、前記ランダムファイルより得られた前記所定の部分の前記ランダムデータから復号化鍵を作成し、
前記復号化鍵によって、再生された、暗号化された前記情報を復号化することを特徴とする復号化方法。

【請求項２０】　記録媒体に固有の固有情報から作成した第１の暗号化鍵と前記第１の暗号化鍵とは独立の第２の暗号化鍵に基づいて作成された第３の暗号化鍵によって暗号化された情報が記録された前記記録媒体の前記固有情報から、第１の復号化鍵を作成し、
所定の鍵媒体に記録された前記第２の暗号化鍵に対応する第２の復号化鍵と前記第１の復号化鍵に基づいて、第３の復号化鍵を作成し、
前記第３の復号化鍵によって、前記記録媒体から再生された前記第３の暗号化鍵によって暗号化された前記情報を復号化することを特徴とする復号化方法。

【請求項２１】　前記鍵媒体は、前記第２の復号化鍵が磁気的または光学的に記録されているカードであることを特徴とする請求項２０に記載の復号化方法。

【請求項２２】　前記鍵媒体は、前記第２の復号化鍵が記憶されているメモリを備えることを特徴とする請求項２０に記載の復号化方法。

【請求項２３】　記録媒体に固有の固有情報に基づいて暗号化鍵を作成し、前記暗号化鍵に基づいて、前記記録媒体に記録すべき情報を暗号化する暗号化装置において、
前記記録媒体に固有の前記固有情報として前記記録媒体

に形成されたウォブリングされたプリグループまたはランド部の所定の部分の周波数に基づいて、前記暗号化鍵を作成する暗号化鍵作成手段と、
前記暗号化鍵作成手段によって作成された前記暗号化鍵に基づいて、前記記録媒体に記録すべき前記情報を暗号化する暗号化手段とを備えることを特徴とする暗号化装置。

【請求項２４】　記録媒体に固有の固有情報に基づいて暗号化鍵を作成し、前記暗号化鍵に基づいて、前記記録媒体に記録すべき情報を暗号化する暗号化装置において、
前記記録媒体に固有の前記固有情報として、前記記録媒体に記録されるべき暗号化された前記情報の所定の部分に挿入されるランダムデータに基づいて、前記暗号化鍵を作成する暗号化鍵作成手段と、
前記暗号化鍵作成手段によって作成された前記暗号化鍵に基づいて、前記記録媒体に記録すべき前記情報を暗号化する暗号化手段とを備えることを特徴とする暗号化装置。

【請求項２５】　記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるべきランダムデータに基づいて作成された暗号化鍵によって暗号化された前記情報が格納された第１のファイル、および暗号化された前記情報の所定の部分に挿入される前記ランダムデータの所定の部分を示すデータが格納された第２のファイルが記録された前記記録媒体から、前記第１のファイル、および前記第２のファイルを再生する再生手段と、
前記再生手段により再生された前記第２のファイルに格納された、前記ランダムデータの所定の部分を示すデータに基づいて、前記再生手段により再生された前記第１のファイルに格納された暗号化された前記情報から、前記ランダムデータを検出する検出手段と、
前記検出手段により検出された前記ランダムデータから復号化鍵を作成する復号化鍵作成手段と、
前記復号化鍵作成手段により作成された前記復号化鍵によって、前記再生手段により再生された前記第１のファイルの暗号化された前記情報を復号化する復号化手段とを備えることを特徴とする復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化方法および装置並びに復号化方法および装置に関し、例えば、映像信号、音声信号、データ信号等の情報を暗号化するとともに暗号化した情報を復号化する場合に用いて好適な暗号化方法および装置並びに復号化方法および装置に関する。

【０００２】

【従来の技術】従来、所定の記録媒体に情報を暗号化して記録する場合、所定の暗号化キーを用いて情報を暗号化し、暗号化された情報を復号化するための復号化キー

を用いて、暗号化された情報を復号化している。

【０００３】また、「特公平２－６０００７」には、記録媒体に記録すべきファイルを構成するデータに基づいて暗号化キーを作成し、それを用いて暗号化した情報を記録し、上記ファイルを再生し、そのファイルを構成するデータに基づいて復号化キーを作成し、暗号化された情報を復号化するようにした暗号化方法が開示されている。

【０００４】

【発明が解決しようとする課題】しかしながら、従来の暗号化方法および復号化方法においては、暗号化キーを作成するファイルが１箇所（連続領域）に記録されているため、そのファイルが比較的容易にコピーされてしまう可能性がある課題があった。

【０００５】本発明はこのような状況に鑑みてなされたものであり、記録媒体に記録された情報に強力なコピープロテクトを掛けることができるようにするものである。

【０００６】

【課題を解決するための手段】請求項１に記載の暗号化方法は、記録媒体に固有の固有情報は、記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分の周波数であることを特徴とする。

【０００７】請求項３に記載の暗号化方法は、記録媒体に固有の固有情報は、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるランダムデータである。

【０００８】請求項１５に記載の暗号化方法は、記録媒体の固有の情報から作成した第１の暗号化鍵と第１の暗号化鍵とは独立の第２の暗号化鍵から第３の暗号化鍵を作成し、第３の暗号化鍵によって、記録媒体に記録すべき情報を暗号化することを特徴とする。

【０００９】請求項１６に記載の復号化方法は、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるべきランダムデータに基づいて作成された暗号化鍵によって暗号化された情報が格納された第１のファイル、および暗号化された情報の所定の部分に挿入されるランダムデータの所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生し、再生された第２のファイルに格納された、ランダムデータの所定の部分を示すデータに基づいて、再生された第１のファイルに格納された暗号化された情報から、ランダムデータを検出し、検出されたランダムデータから復号化鍵を作成し、復号化鍵によって、再生された第１のファイルの暗号化された情報を復号化することを特徴とする。

【００１０】請求項１７に記載の復号化方法は、記録媒体に記録されるべき情報の所定の部分のウォブリング周波数に基づいて作成された暗号化鍵によって暗号化された情報が格納された第１のファイル、および記録媒体に

記録されるべき暗号化された情報の所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生し、再生された第２のファイルに格納された、暗号化された情報の所定の部分を示すデータに基づいて、再生された第１のファイルに格納された情報の所定の部分のウォブリング周波数を検出し、検出されたウォブリング周波数に基づいて、復号化鍵を作成し、復号化鍵によって、再生された第１のファイルに格納された、暗号化された情報を復号化することを特徴とする。

【００１１】請求項１８に記載の復号化方法は、記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分の周波数に基づいて作成された暗号化鍵によって暗号化された情報が格納された第１のファイルおよび記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイルおよび第２のファイルを再生し、再生された第２のファイルに格納されたウォブリングされたプリグルーブまたはランド部の所定の部分を示すデータに基づいて、記録媒体に形成されたプリグルーブまたはランド部の所定の部分のウォブリング周波数を検出し、検出されたウォブリング周波数に基づいて、復号化鍵を作成し、復号化鍵によって、再生された第１のファイルに格納された暗号化された情報を復号化することを特徴とする。

【００１２】請求項１９に記載の復号化方法は、所定の記録媒体に記録された、所定の疑似ランダム発生器によって作成されたランダムデータからなるランダムファイルの所定の部分から選択されたランダムデータに基づいて作成された暗号化鍵によって暗号化された情報が格納されたファイル、ランダムデータからなるランダムファイルの所定の部分を示すデータが格納されたファイル、およびランダムファイルを再生し、再生されたランダムファイルの所定の部分を示すデータが格納されたファイルに基づいて、ランダムファイルより得られた所定の部分のランダムデータから復号化鍵を作成し、復号化鍵によって、再生された、暗号化された情報を復号化することを特徴とする。

【００１３】請求項２０に記載の復号化方法は、記録媒体に固有の固有情報から作成した第１の暗号化鍵と第１の暗号化鍵とは独立の第２の暗号化鍵に基づいて作成された第３の暗号化鍵によって暗号化された情報が記録された記録媒体の固有情報から、第１の復号化鍵を作成し、所定の鍵媒体に記録された第２の暗号化鍵に対応する第２の復号化鍵と第１の復号化鍵に基づいて、第３の復号化鍵を作成し、第３の復号化鍵によって、記録媒体から再生された第３の暗号化鍵によって暗号化された情報を復号化することを特徴とする。

【００１４】請求項２３に記載の暗号化装置は、記録媒

体に固有の固有情報として記録媒体に形成されたウォブリングされたプリグルーブまたはランド部の所定の部分の周波数に基づいて、暗号化鍵を作成する暗号化鍵作成手段と、暗号化鍵作成手段によって作成された暗号化鍵に基づいて、記録媒体に記録すべき情報を暗号化する暗号化手段とを備えることを特徴とする。

【００１５】請求項２４に記載の暗号化装置は、記録媒体に固有の固有情報として、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるランダムデータに基づいて、暗号化鍵を作成する暗号化鍵作成手段と、暗号化鍵作成手段によって作成された暗号化鍵に基づいて、記録媒体に記録すべき情報を暗号化する暗号化手段とを備えることを特徴とする。

【００１６】請求項２５に記載の復号化装置は、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるべきランダムデータに基づいて作成された暗号化鍵によって暗号化された情報が格納された第１のファイル、および暗号化された情報の所定の部分に挿入されるランダムデータの所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生する再生手段と、再生手段により再生された第２のファイルに格納された、ランダムデータの所定の部分を示すデータに基づいて、再生手段により再生された第１のファイルに格納された暗号化された情報から、ランダムデータを検出する検出手段と、検出手段により検出されたランダムデータから復号化鍵を作成する復号化鍵作成手段と、復号化鍵作成手段により作成された復号化鍵によって、再生手段により再生された第１のファイルの暗号化された情報を復号化する復号化手段とを備えることを特徴とする。

【００１７】請求項１に記載の暗号化方法においては、記録媒体に固有の固有情報を、記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分の周波数とする。

【００１８】請求項３に記載の暗号化方法においては、記録媒体に固有の固有情報を、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるランダムデータとする。

【００１９】請求項１５に記載の暗号化方法においては、記録媒体の固有の情報から作成した第１の暗号化鍵と第１の暗号化鍵とは独立の第２の暗号化鍵から第３の暗号化鍵を作成し、第３の暗号化鍵によって、記録媒体に記録すべき情報を暗号化する。

【００２０】請求項１６に記載の復号化方法においては、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるべきランダムデータに基づいて暗号化鍵を作成し、暗号化鍵によって暗号化された情報が格納された第１のファイル、および暗号化された情報の所定の部分に挿入されるランダムデータの所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生し、再生された第２のファイルに格納された、ランダムデータの所定の部分を示すデータに基づいて、再生された第１のファイルに格納された暗号化された情報から、ランダムデータを検出し、検出されたランダムデータから復号化鍵を作成し、復号化鍵によって、再生された第１のファイルの暗号化された情報を復号化する。

【００２１】請求項１７に記載の復号化方法においては、記録媒体に記録されるべき情報の所定の部分のウォブリング周波数に基づいて暗号化鍵を作成し、暗号化鍵によって暗号化された情報が格納された第１のファイル、および記録媒体に記録されるべき暗号化された情報の所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生し、再生された第２のファイルに格納された、暗号化された情報の所定の部分を示すデータに基づいて、再生された第１のファイルに格納された情報の所定の部分のウォブリング周波数を検出し、検出されたウォブリング周波数に基づいて、復号化鍵を作成し、復号化鍵によって、再生された第１のファイルに格納された、暗号化された情報を復号化する。

【００２２】請求項１８に記載の復号化方法においては、記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分の周波数に基づいて、暗号化鍵を作成し、暗号化鍵によって暗号化された情報が格納された第１のファイルおよび記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイルおよび第２のファイルを再生し、再生された第２のファイルに格納されたウォブリングされたプリグルーブまたはランド部の所定の部分を示すデータに基づいて、記録媒体に形成されたプリグルーブまたはランド部の所定の部分のウォブリング周波数を検出し、検出されたウォブリング周波数に基づいて、復号化鍵を作成し、復号化鍵によって、再生された第１のファイルに格納された暗号化された情報を復号化する。

【００２３】請求項１９に記載の復号化方法においては、所定の疑似ランダム発生器によって作成されたランダムデータからなるランダムファイルの所定の部分から選択されたランダムデータに基づいて、暗号化鍵を作成し、所定の記録媒体に記録された、暗号化鍵によって暗号化された情報が格納されたファイル、ランダムデータからなるランダムファイルの所定の部分を示すデータが格納されたファイル、およびランダムファイルを再生し、再生されたランダムファイルの所定の部分を示すデータが格納されたファイルに基づいて、ランダムファイルより得られたその部分のランダムデータから復号化鍵を作成し、復号化鍵によって、再生された、暗号化された情報を復号化する。

【００２４】請求項２０に記載の復号化方法においては、記録媒体に固有の固有情報から作成した第１の暗号化鍵と第１の暗号化鍵とは独立の第２の暗号化鍵に基づいて作成された第３の暗号化鍵によって暗号化された情報が記録された記録媒体の固有情報から、第１の復号化鍵を作成し、所定の鍵媒体に記録された第２の暗号化鍵に対応する第２の復号化鍵と第１の復号化鍵に基づいて、第３の復号化鍵を作成し、第３の復号化鍵によって、記録媒体から再生された第３の暗号化鍵によって暗号化された情報を復号化する。

【００２５】請求項２３に記載の暗号化装置においては、暗号化鍵作成手段は、記録媒体に固有の固有情報として記録媒体に形成されたウォブリングされたプリグルーブまたはランド部の所定の部分の周波数に基づいて、暗号化鍵を作成し、暗号化手段は、暗号化鍵作成手段によって作成された暗号化鍵に基づいて、記録媒体に記録すべき情報を暗号化する。

【００２６】請求項２４に記載の暗号化装置においては、暗号化鍵作成手段が、記録媒体に固有の固有情報として、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるランダムデータに基づいて、暗号化鍵を作成し、暗号化手段が、暗号化鍵作成手段によって作成された暗号化鍵に基づいて、記録媒体に記録すべき情報を暗号化する。

【００２７】請求項２５に記載の復号化装置においては、再生手段が、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるべきランダムデータに基づいて作成された暗号化鍵によって暗号化された情報が格納された第１のファイル、および暗号化された情報の所定の部分に挿入されるランダムデータの所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生し、検出手段が、再生手段により再生された第２のファイルに格納された、ランダムデータの所定の部分を示すデータに基づいて、再生手段により再生された第１のファイルに格納された暗号化された情報から、ランダムデータを検出し、復号化鍵作成手段が、検出手段により検出されたランダムデータから復号化鍵を作成し、復号化手段が、復号化鍵作成手段により作成された復号化鍵によって、再生手段により再生された第１のファイルの暗号化された情報を復号化する。

【００２８】

【発明の実施の形態】以下に、本発明の実施例を説明するが、その前に、特許請求の範囲に記載の発明の各手段と以下の実施例との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施例（但し、一例）を付加して、本発明の特徴を記述すると、次のようになる。

【００２９】即ち、請求項２３に記載の暗号化装置は、記録媒体に固有の固有情報として記録媒体に形成されたウォブリングされたプリグルーブまたはランド部の所定の部分の周波数に基づいて、暗号化鍵を作成する暗号化鍵作成手段（例えば、図１の暗号化鍵発生部４）と、暗号化鍵作成手段によって作成された暗号化鍵に基づいて、記録媒体に記録すべき情報を暗号化する暗号化手段（例えば、図１の暗号化部３）とを備えることを特徴とする。

【００３０】請求項２４に記載の暗号化装置は、記録媒体に固有の固有情報として、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるランダムデータに基づいて、暗号化鍵を作成する暗号化鍵作成手段（例えば、図１の暗号化鍵発生部４）と、暗号化鍵作成手段によって作成された暗号化鍵に基づいて、記録媒体に記録すべき情報を暗号化する暗号化手段（例えば、図１の暗号化部３）とを備えることを特徴とする。

【００３１】請求項２５に記載の復号化装置は、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるべきランダムデータに基づいて作成された暗号化鍵によって暗号化された情報が格納された第１のファイル、および暗号化された情報の所定の部分に挿入されるランダムデータの所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生する再生手段（例えば、図１の再生部１６）と、再生手段により再生された第２のファイルに格納された、ランダムデータの所定の部分を示すデータに基づいて、再生手段により再生された第１のファイルに格納された暗号化された情報から、ランダムデータを検出する検出手段（例えば、図１の復号鍵作成部１８）と、検出手段により検出されたランダムデータから復号化鍵を作成する復号化鍵作成手段（例えば、図１の復号鍵作成部１８）と、復号化鍵作成手段により作成された復号化鍵によって、再生手段により再生された第１のファイルの暗号化された情報を復号化する復号化手段（例えば、図１の復号化部１７）とを備えることを特徴とする。

【００３２】なお、勿論この記載は、各手段を上記したものに限定することを意味するものではない。

【００３３】以下に、本発明の実施例について説明する。実施例で使用される情報は、映像情報、音声情報、テキスト情報等である。また、復号化の対象となる暗号化された情報が記録される記録媒体としては、例えば、ＤＶＤ（デジタル・バーサタイル・ディスク：Digital Versatile Disc）、光ディスク、光磁気ディスク、およびフロッピディスクやハードディスク等の磁気ディスクなどのディスク状の記録媒体、あるいは磁気テープ等のテープ状の記録媒体が可能である。

【００３４】これらの記録媒体は、マスタディスクやマスタ磁気テープ等から多数複製されたスレーブ記録媒体である。暗号化方法としては、符号化、スクランブル、シャフリング、ＭＰＥＧ（Moving Picture Experts Gro

up）方式によるエンコード、ＪＰＥＧ（Joint Photographic Experts Group）方式によるエンコード等が可能であり、それに対応して、復号化方法としては、デスクランブル、デシャフリング、ＭＰＥＧ方式によるデコード、ＪＰＥＧ方式によるデコード等が可能となる。

【００３５】図１は、本発明の暗号化装置および復号化装置の構成例を示すブロック図である。

【００３６】暗号化装置１において、情報データ発生部２は、情報データ（例えば、デジタル映像情報、デジタル音声情報等）が記録された磁気テープ等から、その情報データを再生する再生装置等からなり、再生した情報データ（平文）を出力するようになされている。暗号化部３は、情報データ発生部２からの情報データを暗号化し、暗号化された情報データ（暗号文）を出力するようになされている。

【００３７】固有情報発生部５は、記録媒体固有の情報を出力するようになされている。この記録媒体固有の情報にはランダムデータ（乱数データ）等が用いられ、後述する記録部７によって、ディスク等の記録媒体の所定の領域に、例えば、図２に示したように、ＩＳＯ９６６０の通常のファイル（normal file）として記録されるようになされている。通常のファイルなので、コピーすることは可能であるが、ハードディスク等の記録媒体にコピーされた場合、ファイルの位置（アロケーション）が変化するため、オリジナルディスクと同一の情報を得ることはできない。

【００３８】図２は、ＩＳＯ９６６０のロジカルファイルフォーマットを示しており、０セクタ（ｓｅｃ）乃至１４９セクタは、プレギャップ（pre gap）とされ、データは入れても入れなくともよい。１５０セクタ乃至１６５セクタは、システムエリア（system area）とされ、例えば、コピーライト情報が格納される。次の、１６６セクタ乃至ｎ－１セクタ（ここで、ｎは可変であり、所定の整数値である）は、ボリュームデスクリプタ（volume descriptors）とされ、マネージメント情報が格納される。

【００３９】ボリュームデスクリプタには、プライマリボリュームデスクリプタ（primaryvolume descriptor）が置かれ、ディレクトリの一覧（パステーブル）等が格納される。ｎセクタより以降は、ユーザがアクセスできる領域であり、所定のファイルが格納される。各セクタの大きさは２キロバイトであり、その中の位置を示すために、オフセットが用いられる。

【００４０】また、例えば、図２に示したように、ランダムデータを通常のファイルであるがインタリーブされたファイル（interleaved file）に記録するようにすることができる。あるいは、通常のファイルであるが、マルチエクステントされたファイル（multi extent file）に記録するようにすることができる。ここで、インタリーブされたファイルとは、図２に示したように、所定の連続領域内において、不連続な複数の部分にランダムデータを記録するようにしたファイルのことであり、マルチエクステントファイルとは、複数の不連続な領域にランダムデータを記録して１つのファイルを構成するようにしたファイルのことである。

【００４１】ファイルをインタリーブあるいはマルチエクステントにすることにより、ランダムデータの位置を分散させることができ、読み出し専用のディスク上に記録されたランダムデータの位置と、そこに記録されたランダムデータをハードディスク上にコピーした場合におけるそのランダムデータのハードディスク上での位置とを同一にすることがより困難となる。

【００４２】また、ランダムデータをＩＳＯ９６６０のプリギャップエリア（pre gap）（００：００：００：００乃至００：００：０２：００）、あるいは、システムエリア（sysytem area）（００：００：０２：００乃至００：００：０２：１６）に記録するようにすることもできる。これらのエリアに記録することにより、通常のファイルとしてアクセスすることができないため、コピーすることが困難になる。

【００４３】さらに、ランダムデータをＩＳＯ９６６０のボリュームディスクリプタ（volume descriptors）の中の、プライマリボリュームデスクリプタ（primary volumedescriptor）のオフセットが８８４バイト目から１３９５バイト目までのアプリケーションエリア（application area）に記録するようにすることもできる。このエリアは、ＩＳＯ９６６０のファイルのヘッダ情報であるので、通常のファイルとしてはアクセスすることができない。そのためコピーすることが困難になる。

【００４４】そして、ランダムデータは最終的にはマスタディスク１２上に記録されるようになされている。

【００４５】ファイル形成部６は、暗号化された情報データの所定部分を示すファイルを形成するようになされている。即ち、上記暗号化された情報データに挿入されてマスタディスク１２に記録されるランダムデータの同一セクタまたは異なるセクタ内のそれぞれ所定バイト目から他の所定バイト目までのランダムデータを指定する、１組または複数組のセクタ番号およびオフセット（セクタ内のバイト番号）からなるファイル（ダイジェストメソッドファイル）を形成する。そして、この情報データの所定部分を示すファイルも、暗号化された情報データの中の予め決められたエリアに挿入して、最終的には、マスタディスク１２に記録されるようになされている。

【００４６】記録部７は、固有情報発生部５からのランダムデータおよびファイル形成部６からのダイジェストメソッドファイル、および暗号化部３からの暗号化された情報データをハードディスク８に記録する。再生部９は、磁気ヘッド、増幅器等で構成され、ハードディスク８に記録されたダイジェストメソッドファイルに基づい

て、ランダムデータを読み出し、暗号化鍵発生部４に供給するとともに、暗号化された情報データを読み出し、フォーマット化部１０に供給するようになされている。

【００４７】フォーマット化部１０は、再生部９からの暗号化された情報データやダイジェストメソッドファイルをフォーマット化し、プリマスタイメージを作成し、記録部７に供給するようになされている。このとき、ファイルのフォーマットを、例えば、上述したように、インタリーブあるいはマルチエクステントにすることができる。記録部７は、プリマスタイメージをハードディスク８に記録するようになされている。記録部１１は、光学ヘッド、増幅器等からなり、再生部９によってハードディスク８より再生されたプリマスタイメージを、マスタディスク１２に記録するようになされている。ディスク再生装置１３は、このマスタディスク１２を原盤として、多数のディスク１５（スレーブディスク）を複製するようになされている。

【００４８】復号化装置１４において、再生部１６は、ディスク１５を再生するようになされている。復号化鍵作成部１８は、再生部１６からの再生信号に基づいて、復号化鍵を作成し、出力するようになされている。復号化部１７は、復号化鍵作成部１８より供給される復号化鍵に基づいて、再生部１６より供給される再生信号を復号化するようになされている。

【００４９】次に、図３のフローチャートを参照して、暗号化装置１における暗号化の動作について説明する。最初に、ステップＳ１において、ファイル形成部６は、記録媒体の固有値（暗号化鍵）を得るための乱数データ（ランダムデータ）を、マスタディスク１２のどの領域から抽出するかを決定し、決定した１つまたは複数の領域を示すファイル（ダイジェストメソッドファイル）を作成する。

【００５０】このダイジェストメソッドファイルは、例えば、図４に示すように、セクタ番号１乃至セクタ番号ｎ（ここで、ｎは数十程度である）のｎ個のセクタの多数のオフセット（オフセット番号）のテーブルからなり、図５に示すように、そのうちの例えば、セクタ番号１のセクタ内の所定のオフセットから他の所定のオフセットまでと、セクタ番号２のセクタ内の所定のオフセットから他の所定のオフセットまでが指定されたものであり、記録部７を介してハードディスク８に記録される。

【００５１】次に、ステップＳ２に進み、再生部９は、ステップＳ１において決定されたダイジェストメソッドファイルのセクタ番号１のセクタ内の所定のオフセットから他の所定のオフセットまでと、セクタ番号２のセクタ内の所定のオフセットから他の所定のオフセットまでの、ハードディスク８に記録されているランダムデータ（乱数データ）を再生し、それらを集める。集められたこれらのランダムデータは、暗号化鍵発生部４に供給される。

【００５２】次に、ステップＳ３において、暗号化鍵発生部４は、再生部９より供給されたランダムデータに対して所定の演算を施し、図５に示したように、暗号化鍵（固有値）（ディスクダイジェスト）を作成する。この暗号化鍵は暗号化部３に供給され、暗号化部３において、この暗号化鍵に基づいて、情報データ発生部２より供給される情報データが暗号化される。暗号化された情報データは、記録部７に供給され、記録部７によってハードディスク８に記録される。

【００５３】次に、ステップＳ４に進み、ハードディスク８に記録された暗号化された情報データ、記録媒体固有の情報および暗号化された情報データの所定部分を示すダイジェストメソッドファイルが、再生部９によって再生され、フォーマット化部１０に供給される。フォーマット化部１０は、再生部９より供給されたこれらの暗号化された情報データ、記録媒体固有の情報および暗号化された情報データの所定部分を示すダイジェストメソッドファイルから、プリマスタイメージ（フォーマット化信号）を作成する。このとき、上述したように、ファイルのフォーマットをインタリーブあるいはマルチエクステントにして分散させることが可能である。

【００５４】作成したプリマスタイメージは、記録部７に供給され、記録部７によって一旦ハードディスク８に記録される。ハードディスク８に記録されたプリマスタイメージは、再生部９によって再生され、再生データが記録部１１に供給される。記録部１１は、再生部９からの再生データをマスタディスク１２に記録する。あるいは、フォーマット化部１０からのプリマスタイメージ、即ち、フォーマット化信号を直接、記録部１１に供給し、記録部１１がそれをマスタディスク１２に記録するようにすることも可能である。

【００５５】このようにして作成されたマスタディスク１２を原盤として、ディスク作成装置１３によって多数のディスク（スレーブディスク）（ＤＶＤ、光ディスク、光磁気ディスク等）１５が複製される。なお、記録媒体として磁気テープを用いる場合には、転写装置を用いて、マスタ磁気テープに記録された記録信号を多数のスレーブ磁気テープに転写するようにすればよい。

【００５６】次に、図６に示したフローチャートを参照して、復号化装置１４における復号化の動作について説明する。最初、ステップＳ１１において、再生部１６により、ディスク１５の記録信号が再生される。この再生信号は、復号化鍵作成部１８からのゲート信号が再生部１６に供給されることにより、その再生信号のうちの暗号化された情報データが復号化部１７に供給され、再生信号のうちのランダムデータのファイルおよびダイジェストメソッドファイルが復号化鍵作成部１８に供給される。

【００５７】次に、ステップＳ１２に進み、暗号化鍵作成部１８は、再生部１６より供給されたランダムデータ

のうち、ダイジェストメソッドファイルによって指定された例えばセクタ番号１のセクタ内の所定のオフセットから他の所定のオフセットまでと、セクタ番号２のセクタ内の所定のオフセットから他の所定のオフセットまでのランダムデータを抽出し、集める。

【００５８】次に、ステップＳ１３において、ステップＳ１２において集められたランダムデータに対して所定の演算（例えば、加算演算）を行ったもの、またはランダムデータ自体から、元の暗号化鍵に対応する復号化鍵を作成し、復号化部１７に供給する。ステップＳ１４においては、復号化部１７により、復号化鍵作成部１８より供給された復号化鍵に基づいて、再生部１６より供給された再生データ、即ち、暗号化された情報データ（暗号文）が復号され、元の情報データ（平文）にされた後、出力端子１９より出力される。

【００５９】上記暗号化装置１においては、マスタディスク１２のトラックに、記録信号のピットの列をウォブリング状に記録する場合には、上記ランダムデータに代えて、マスタディスク１２に記録される記録信号のピットの列のウォブリングを示すウォブリング信号を、また、記録媒体としてのディスク１５に固有の情報が、ディスク１５に形成されるべき物理的情報である場合において、マスタディスク１２の記録信号が記録されるトラックが、ウォブリングされたプリグルーブ若しくはウォブリングされたランド部であるとき、そのプリグルーブまたはランド部に対応するウォブリング信号を、記録媒体に固有の情報信号として固有情報発生部５から発生させるようにしてもよい。

【００６０】そして、暗号化鍵発生部４は、このウォブリング信号に基づいて暗号化鍵を発生し、暗号化部３に供給する。暗号化部３は、暗号化鍵発生部４より供給される暗号化鍵に基づいて、情報データ発生部２からの情報データを暗号化する。

【００６１】その場合には、復号化装置１４において、復号化鍵作成部１８は、ディスク１５の記録信号の所定の部分のプリグルーブ、またはランド部のウォブリング周波数を検出し、そのウォブリング周波数に対応するデータに対して所定の演算を施したもの、またはウォブリング周波数に対応するデータ自体に基づいて、元の暗号化鍵に対応する復号化鍵を作成し、復号化部１７に供給する。そして、復号化部１７は、復号化鍵作成部１８より供給された復号化鍵を用いて、再生部１６より供給される暗号化された情報データ（暗号文）を元の情報データ（平文）に復号する。

【００６２】なお、上述したように、記録媒体に固有の情報が、記録媒体に記録されるべき物理的情報、例えば、記録媒体のウォブリングされたプリグルーブまたはランド部である場合、記録媒体としては、ある程度の厚みがあり、比較的固い基板を有するディスク、例えば、ＤＶＤ、光ディスク、光磁気ディスク、あるいはハードディスク等を用いることができる。

【００６３】図７は、本発明の暗号化および復号化方法を適用した暗号化装置および復号化装置の他の実施例の構成を示すブロック図である。図７に示した暗号化装置１においては、図１に示した暗号化装置において、固有情報発生部５の代わりにランダムファイル形成部２０が設けられ、暗号化された情報の所定部分を示すファイル形成部６の代わりにランダムファイルの所定部分を示すファイル形成部２１が設けられている。その他の構成および動作は、図１に示した暗号化装置および復号化装置の場合と同様であるので、ここではその説明は省略する。

【００６４】次に、図８のフローチャートを参照して、その動作について説明する。暗号化装置１においては、最初、ステップＳ２１において、ランダムファイル形成部２０が、図示せぬ疑似ランダム発生器からランダムデータを発生させ、例えば数キロバイト以上のランダムデータを含むランダムファイルを作成する。作成したランダムファイルは、記録部７に供給され、記録部７によってハードディスク８に記録される。

【００６５】次に、ステップＳ２２に進み、固有値（暗号鍵）を得るための乱数データ（ランダムデータ）をランダムファイルのどの部分から集めるかを決定する。即ち、所定のオフセット番号から他のオフセット番号までの１つの所定部分のランダムデータ、または複数の所定部分のランダムデータをランダムデータのどの部分から集めるかを決定する。そして、ファイル形成部２１は、これらのランダムデータの所定部分を示すダイジェストメソッドファイルを形成する。このダイジェストメソッドファイルは、記録部７に供給され、記録部７は、それを一旦ハードディスク８に記録し、最終的には、再生部９によってそれが読み出され、記録部１１により、マスタディスク１２に記録される。

【００６６】次に、ステップＳ２３において、ハードディスク８に記録されている所定のオフセット番地から他の所定のオフセット番地までの１つの所定部分のランダムデータ、または、複数の所定部分のランダムデータを集め、そのランダムデータを再生部９によって再生し、暗号化鍵発生部４に供給し、ランダムデータ自体、またはそれらのランダムデータに所定の演算を施したものから、暗号化鍵（固有値）（ディスクダイジェスト）を作成する。

【００６７】次に、ステップＳ２４に進み、ランダムファイルがマスタディスク１２のどこに配置されるか、即ち、ハードディスク８に記録されている暗号化された情報データにランダムファイルが挿入されてマスタディスク１２に記録されたときの所定のセクタ番号のオフセット値（オフセット番号）を算出し、そのオフセット値をダイジェストメソッドファイルで指定されたオフセット番号（オフセット値）に足し込む。このようにして、ダ

イジェストメソッドファイルを修正する。

【0068】ステップS25においては、暗号化鍵発生部4において作成された暗号化鍵（固有値）（ディスクダイジェスト）が、暗号化部3に供給され、情報データ発生部2からの情報データが暗号化される。暗号化された情報データは、記録部7に供給され、記録部7によってハードディスク8に記録される。

【0069】次に、ステップS26に進み、ハードディスク8に記録されている暗号化された情報データ、記録媒体固有の情報信号、および暗号化された所定部分を示すダイジェストメソッドファイルが再生部9により再生され、フォーマット化部10に供給され、そこでフォーマット化された後、プリマスタイメージが作成される。そのとき、上述したように、ランダムファイルをインタリーブ、あるいはマルチエクステントにすることにより、ランダムファイルを分散させることができる。

【0070】作成されたプリマスタイメージは、記録部7により一旦ハードディスク8に記録される。ハードディスク8に記録されたプリマスタイメージは、再生部9により再生され、再生部9から記録部11に供給されたプリイマスタメージ、またはフォーマット化部10から直接、記録部11に供給されたプリマスタイメージは、記録部9により、マスタディスク12に記録される。

【0071】そして、このマスタディスク12を原盤として、ディスク作成装置13により、多数のディスク（スレーブディスク）15が複製される。

【0072】次に、図9に示したフローチャートを参照して、復号化装置14における復号化の動作について説明する。最初、ステップS31において、再生部16により、ディスク15が再生され、再生データが復号化鍵作成部18に供給される。次に、ステップS32に進み、復号化鍵作成部18により、再生された暗号化された情報データの中の、ダイジェストメソッドファイルによって指定された所定のセクタ番号のセクタの中の所定のオフセットから他の所定のオフセットまでと、これとは異なる所定のオフセットから他の所定のオフセットまでのランダムデータが抽出され、集められる。

【0073】次に、ステップS33において、このランダムデータに対して所定の演算を施したもの、またはこのランダムデータ自体に基づいて、元の暗号化鍵に対応する復号化鍵が作成され、作成された復号化鍵が復号化部17に供給される。ステップS34においては、復号化部17により、復号化鍵作成部18より供給された復号化鍵を用いて、再生部16より供給される暗号化された情報データ（暗号化文）が元の情報データ（平文）に復号され、出力端子19より出力される。

【0074】図10は、本発明の暗号化装置および復号化装置のさらに他の実施例の構成を示すブロック図である。暗号化装置1の構成は、図1を参照して説明した場合と基本的に同様であるので、ここではその説明は省略する。

【0075】次に、図11のフローチャートを参照して、図10に示した暗号化装置1における暗号化方法について説明する。最初、ステップS41において、ユーザに対して配付する配付鍵（配付鍵データ）を適当に定め、暗号化鍵発生部4内のメモリ（例えば、半導体メモリ）に登録する。なお、メモリの代わりにCPU（メモリを含む場合もある）に登録するようにしてもよい。

【0076】次に、ステップS42に進み、図3のフローチャートを参照して上述した場合と同様にして、ディスク15に固有の情報を集め、所定の演算を施すことにより、ディスクダイジェスト（鍵）を作成する。次に、ステップS43において、ステップS41において定められた配付鍵、およびステップS42において作成されたディスクダイジェストに対して所定の演算、例えば排他的論理和演算を施し、それによって得られた演算結果をワーク鍵とする。

【0077】ステップS44においては、ステップS43において演算されたワーク鍵を暗号化鍵として暗号化部3に供給する。暗号化部3は、この暗号化鍵に基づいて、情報データを暗号化する。その後、暗号化部3によって暗号化された情報データは、記録部7に供給され、記録部7によってハードディスク8に記録される。

【0078】図10に示した復号化装置14においては、図1に示した復号化装置14において、鍵読取部22と鍵媒体23を新たに設けるようにしている。鍵媒体23は、上記配付鍵を配付することができるようになされており、例えば配付鍵がアラビア数字、アルファベット、記号、バーコード、あるいはバーコードに類するその他のコード等で印刷されたものでよく、その鍵媒体23は、カードやディスク15自体とすることができる。

【0079】また、鍵媒体23は、配付鍵が記憶されている半導体メモリ等のメモリ、またはメモリを含むCPU等を備えているものでもよい。そして、このメモリまたはCPUを備える鍵媒体23はカード（例えばICカード）等とすることができる。また、鍵媒体23は、配付鍵が磁気的または光学的に記録されたものであってもよい。そして、このような鍵媒体23は、ディスク15を再生する再生装置と一緒に、または単独で販売される。鍵読取部22は、鍵媒体23に印刷または記録された配付鍵を読み出すようになされている。

【0080】次に、図12を参照して、図10に示した復号化装置14の動作について説明する。最初に、ステップS51において、鍵読取部22は、鍵媒体23に印刷または記録された配付鍵を読み出し、復号化鍵作成部18に供給する。次に、ステップS52に進み、復号化鍵作成部18は、図6のフローチャートを参照して上述した場合と同様にして、ディスク15に固有の情報を集めて、それらに対して所定の演算を施し、元のディスクダイジェスト（鍵）に対応するディスクダイジェスト

（鍵）を得る。

【００８１】次に、ステップＳ５３において、復号化鍵作成部１８は、ステップＳ５１において得られた配付鍵と、ステップＳ５２において得られたディスクダイジェストの間で所定の演算、例えば排他的論理和演算を施し、ワーク鍵とする。ステップＳ５４においては、ステップＳ５３において得られたワーク鍵を復号化鍵とし、復号化部１７に供給する。復号化部１７は、復号化鍵作成部１８より供給された復号化鍵を用いて、再生部１６からの暗号化された情報データを復号化し、出力端子１９より出力する。

【００８２】図１３は、図１０に示した暗号化装置および復号化装置における暗号化方法および復号化方法を表した図である。即ち、平文は、配付鍵とディスクダイジェストに基づいて暗号化され、暗号化された暗号文がディスクに記録される。一方、配付鍵は、ディスクとは別の経路でユーザに供給される。ディスクから読み出された暗号文は、配付鍵とディスクの所定の１つまたは複数の領域から読み出されたデータより演算されたディスクダイジェストに基づいて復号化され、復号化された平文が出力される。

【００８３】図１４は、本発明の暗号化装置および復号化装置のさらに他の実施例の構成を示すブロック図である。

【００８４】図１４に示した暗号化装置１は、図１０に示した暗号化装置１において、固有情報発生部５およびファイル形成部６を、図７に示したランダムファイル形成部２０およびランダムファイルの所定部分を示すファイル形成部２１にそれぞれ置き換えるようにしている。ランダムファイル形成部２０およびファイル形成部２１の動作は、図７を参照して上述した場合と基本的に同様であり、その他の各部の動作も、図１０を参照して上述した場合と基本的に同様であるので、ここではその説明は省略するが、このような構成の暗号化装置１および復号化装置１４によっても、図１３に示したような方法で、平文の暗号化、および平文が暗号化された暗号文の復号化を行うことができる。

【００８５】上記各実施例に示した暗号化装置を用いて、所定の記録媒体（この場合、ディスク１５）から情報データ（ファイル）を読み出し、それを所定の記録媒体にダビング（またはコピー）したとしても、ダビング（コピー）先の他の記録媒体上での情報データの位置（アロケーション）は、ダビング（コピー）元のオリジナルの記録媒体上での情報データが記録されていた位置とは通常の場合異なるので、オリジナルの記録媒体と同一の情報を得ることができない。このため、暗号化された情報データを復号化することができないか、または、復号化されて得られた情報データを、特にディジタル信号の状態で出力端子より出力することができない。これにより、コピーを困難にすることができる。

【００８６】また、ランダムファイルをインタリーブ、あるいはマルチエクステントにすることによって、記録媒体に分散して記録することにより、上述したように、読み出し専用のディスク上に記録されたランダムデータの位置と、そこに記録されたランダムデータをハードディスク上にコピーした場合におけるそのランダムデータのハードディスク上での位置とを同一にすることがより困難となる。これにより、不正なダビング（コピー）を抑制することができる。

【００８７】また、上記各実施例において、図１５に示すように、ディスク１５に固有の情報を、例えばＵＶ（紫外）レーザ等により、ディスク表面、即ち、ディスク基板３３の表面に焼き付けるようにすることも可能である。

【００８８】このようにしてディスク基板３３の表面に焼き付けられたディスク固有の情報を読み出すためには、図示せぬ光学ヘッドをディスク面に対して垂直な方向に移動させるなどして、ディスク基板３３の表面に光を集光させるようにする必要があり、特殊な読み出し装置および読み出しコマンド（例えば、光学ヘッドをディスク面に対して垂直な方向に移動させるためのコマンドなど）を必要とする。そのため、この情報の読み出しは困難となり、容易にコピーすることができなくなる。

【００８９】また、この方法は、光学的コピーあるいはいわゆる「はがしコピー」にも対応することができる。ここで、「はがしコピー」とは、図１５において、保護膜３１をディスク基板３３からはがし、ディスク基板３３に形成されたピット３２を物理的にコピーすることである。即ち、ディスクに固有の情報は、ディスク基板３３の表面に焼き付けられているため、ディスク基板３３のピット３２に光を照射し、その反射光または透過光に基づいてピット３２をコピーする光学的コピーや、上記「はがしコピー」によって、ディスク固有の情報がコピーされないようにすることができる。

【００９０】なお、上記各実施例は、有線通信（例えば、電気ケーブル、光ファイバケーブル等による通信）、無線通信（電波、光、音波等による通信）等の通信に利用することができる。その場合には、暗号化装置１において暗号化された暗号文は、有線通信、無線通信を介して復号化装置１４に供給される。

【００９１】また、上記実施例においては、ファイルフォーマットをＩＳＯ－９６６０として説明したが、これに限定されるものではない。

【００９２】

【発明の効果】請求項１に記載の暗号化方法、および請求項２３に記載の暗号化装置によれば、記録媒体に固有の固有情報を、記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分の周波数とするようにしたので、情報に対して強力なコピープロテクトを掛けることができる。

【００９３】請求項３に記載の暗号化方法、および請求項２４に記載の暗号化装置によれば、記録媒体に固有の固有情報を、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるランダムデータとするようにしたので、ランダムデータの挿入位置を分散させるなどして、ランダムデータの読み出しを困難にすることができ、情報に対して強力なコピープロテクトを掛けることが可能となる。

【００９４】請求項１５に記載の暗号化方法によれば、記録媒体の固有の情報から作成した第１の暗号化鍵と第１の暗号化鍵とは独立の第２の暗号化鍵から第３の暗号化鍵を作成し、第３の暗号化鍵によって、記録媒体に記録すべき情報を暗号化するようにしたので、暗号化のための装置の構成を簡単にすることができ、情報に対して強力なコピープロテクトを掛けることができる。

【００９５】請求項１６に記載の復号化方法、および請求項２５に記載の復号化装置によれば、記録媒体に記録されるべき暗号化された情報の所定の部分に挿入されるべきランダムデータに基づいて暗号化鍵を作成し、暗号化鍵によって暗号化された情報が格納された第１のファイル、および暗号化された情報の所定の部分に挿入されるランダムデータの所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生し、再生された第２のファイルに格納された、ランダムデータの所定の部分を示すデータに基づいて、再生された第１のファイルに格納された暗号化された情報から、ランダムデータを検出し、検出されたランダムデータから復号化鍵を作成し、復号化鍵によって、再生された第１のファイルの暗号化された情報を復号化するようにしたので、強力なコピープロテクトが掛けられた情報を復号化することができる。

【００９６】請求項１７に記載の復号化方法によれば、記録媒体に記録されるべき情報の所定の部分のウォブリング周波数に基づいて暗号化鍵を作成し、暗号化鍵によって暗号化された情報が格納された第１のファイル、および記録媒体に記録されるべき暗号化された情報の所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイル、および第２のファイルを再生し、再生された第２のファイルに格納された、暗号化された情報の所定の部分を示すデータに基づいて、再生された第１のファイルに格納された情報の所定の部分のウォブリング周波数を検出し、検出されたウォブリング周波数に基づいて、復号化鍵を作成し、復号化鍵によって、再生された第１のファイルに格納された、暗号化された情報を復号化するようにしたので、強力なコピープロテクトが掛けられた情報を復号化することができる。

【００９７】請求項１８に記載の復号化方法によれば、記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分の周波数に基づいて、暗号化鍵を作成し、暗号化鍵によって暗号化された情報が格納された第１のファイルおよび記録媒体に形成されるべきウォブリングされたプリグルーブまたはランド部の所定の部分を示すデータが格納された第２のファイルが記録された記録媒体から、第１のファイルおよび第２のファイルを再生し、再生された第２のファイルに格納されたウォブリングされたプリグルーブまたはランド部の所定の部分を示すデータに基づいて、記録媒体に形成されたプリグルーブまたはランド部の所定の部分のウォブリング周波数を検出し、検出されたウォブリング周波数に基づいて、復号化鍵を作成し、復号化鍵によって、再生された第１のファイルに格納された暗号化された情報を復号化するようにしたので、強力なコピープロテクトが掛けられた情報を復号化することができる。

【００９８】請求項１９に記載の復号化方法によれば、所定の疑似ランダム発生器によって作成されたランダムデータからなるランダムファイルの所定の部分から選択されたランダムデータに基づいて、暗号化鍵を作成し、所定の記録媒体に記録された、暗号化鍵によって暗号化された情報が格納されたファイル、ランダムデータからなるランダムファイルの所定の部分を示すデータが格納されたファイル、およびランダムファイルを再生し、再生されたランダムファイルの所定の部分を示すデータが格納されたファイルに基づいて、ランダムファイルより得られたその部分のランダムデータから復号化鍵を作成し、復号化鍵によって、再生された、暗号化された情報を復号化するようにしたので、強力なコピープロテクトが掛けられた情報を復号化することができる。

【００９９】請求項２０に記載の復号化方法によれば、記録媒体に固有の固有情報から作成した第１の暗号化鍵と第１の暗号化鍵とは独立の第２の暗号化鍵に基づいて作成された第３の暗号化鍵によって暗号化された情報が記録された記録媒体の固有情報から、第１の復号化鍵を作成し、所定の鍵媒体に記録された第２の暗号化鍵に対応する第２の復号化鍵と第１の復号化鍵に基づいて、第３の復号化鍵を作成し、第３の復号化鍵によって、記録媒体から再生された第３の暗号化鍵によって暗号化された情報を復号化するようにしたので、強力なコピープロテクトが掛けられた情報を復号化することができる。

【図面の簡単な説明】

【図１】本発明の暗号化装置および復号化装置の実施例の構成を示すブロック図である。

【図２】ＩＳＯ９６６０のロジカルファイルフォーマットを示す図である。

【図３】図１の暗号化装置１の動作を説明するためのフローチャートである。

【図４】ダイジェストメソッドファイルの構成例を示す図である。

【図５】ディスクダイジェストの作成方法を説明するた

めの図である。

【図６】図１の復号化装置１４の動作を説明するためのフローチャートである。

【図７】本発明の暗号化装置および復号化装置の他の実施例の構成を示すブロック図である。

【図８】図７の暗号化装置１の動作を説明するためのフローチャートである。

【図９】図７の復号化装置１４の動作を説明するためのフローチャートである。

【図１０】本発明の暗号化装置および復号化装置のさらに他の実施例の構成を示すブロック図である。

【図１１】図１０の暗号化装置１の動作を説明するためのフローチャートである。

【図１２】図１０の復号化装置１４の動作を説明するためのフローチャートである。

【図１３】図１０に示した暗号化装置１および復号化装

置１４において行われる暗号化および復号化の方法を説明するための図である。

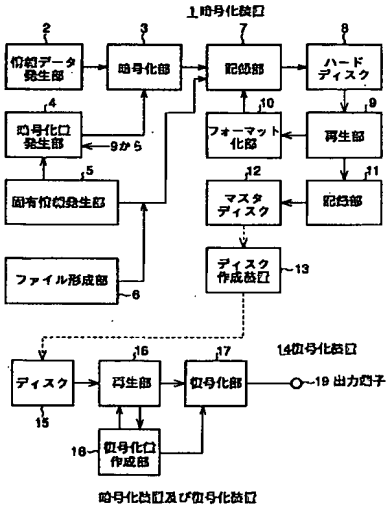
【図１４】本発明の暗号化装置および復号化装置のさらに他の実施例の構成を示すブロック図である。

【図１５】ディスク１５の構造を示す図である。

【符号の説明】

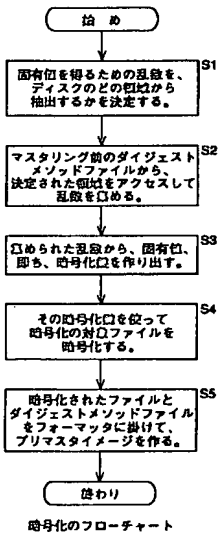
１　暗号化装置，２　情報データ発生部，３　暗号化部，４　暗号化鍵発生部，５　固有情報発生部，６　ファイル形成部，７　記録部，８　ハードディスク，９　再生部，１０　フォーマット化部，１１　記録部，１２　マスタディスク，１３　ディスク作成装置，１４　復号化装置，１５　ディスク，１６　再生部，１７　復号化部，１８　復号化鍵作成部，１９　出力端子，２０　ランダムファイル形成部，２１　ファイル形成部，２２　鍵読取部，２３　鍵媒体，３１保護膜，３２　ピット，３３　ディスク基板

【図１】



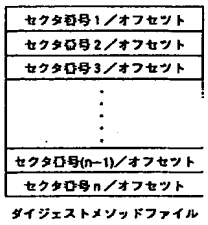
暗号化装置及び復号化装置

【図３】



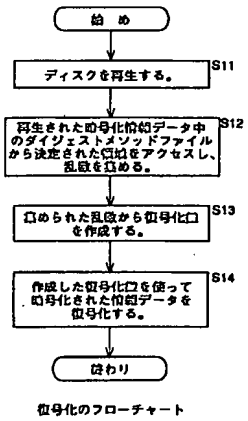
暗号化のフローチャート

【図４】



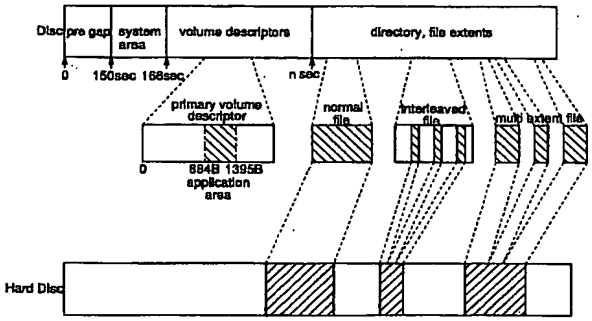
ダイジェストメソッドファイル

【図６】

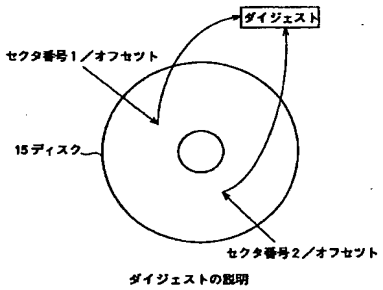


復号化のフローチャート

【図2】

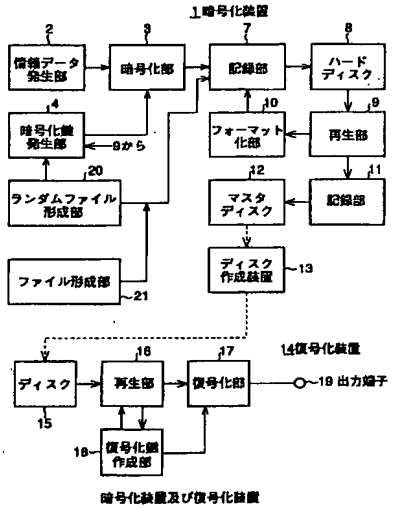


【図5】



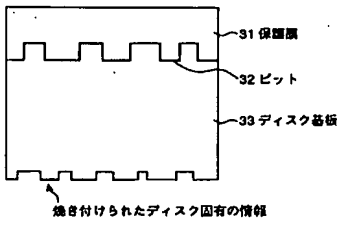
ダイジェストの説明

【図7】

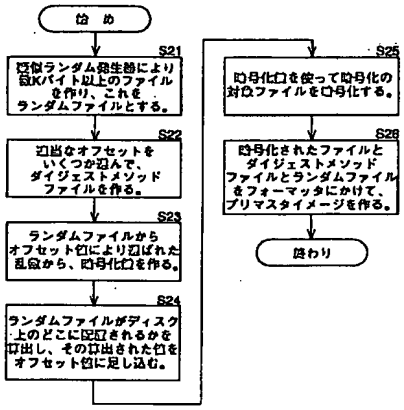


暗号化装置及び復号化装置

【図15】

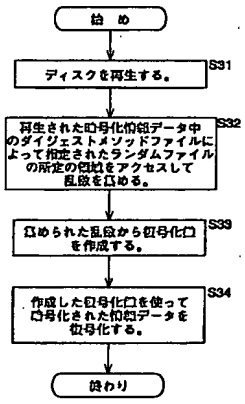


【図８】



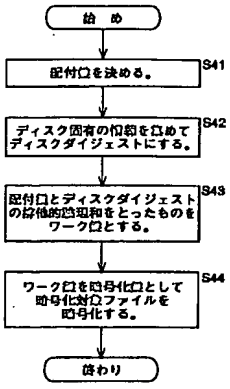
暗号化のフローチャート

【図９】



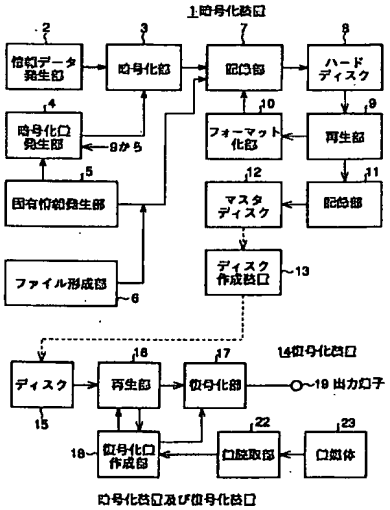
位号化のフローチャート

【図１１】



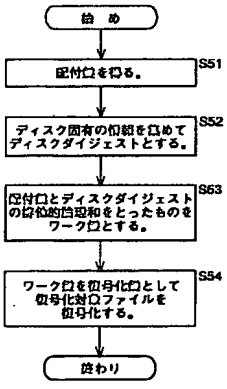
暗号化のフローチャート

【図１０】



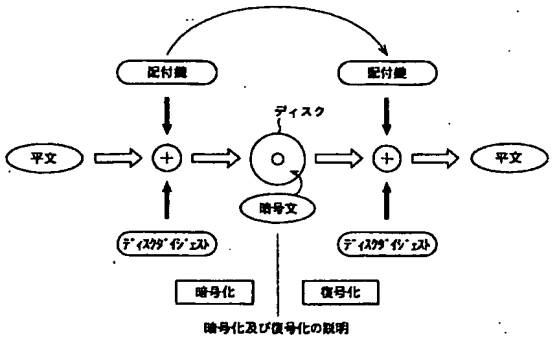
暗号化装口及び位号化装口

【図１２】

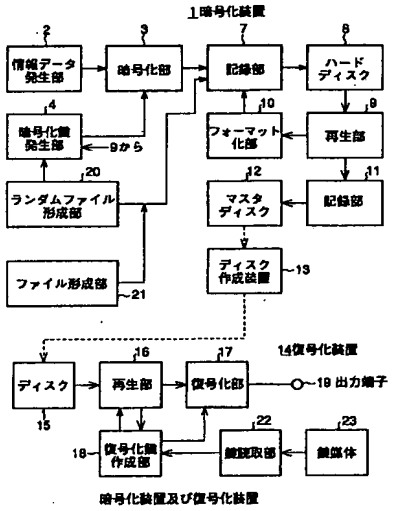


位号化のフローチャート

【図１３】



【図１４】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	FI		技術表示箇所
G11B 20/10		7736－5D	G11B 20/10	H	
// H04L 9/10			H04L 9/00	621Z	